UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/674,940	09/29/2003	Gabriel Montenegro	SUN-P9109	5180

57960 7590 11/26/2007

SUN MICROSYSTEMS INC.
C/O PARK, VAUGHAN & FLEMING LLP
2820 FIFTH STREET
DAVIS, CA 95618-7759

EXAMINER	
LASHLEY, LAUREL L	
ART UNIT	**PAPER NUMBER**
2132	
MAIL DATE	**DELIVERY MODE**
11/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/674,940	Applicant(s) MONTENEGRO ET AL.	
	Examiner Laurel Lashley	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 14 September 2007.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-27 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-27 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 09/14/2007 has been entered.

Claim Rejections - 35 USC § 103

2. Claims 1 – 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Immonen in US PGPub No. 2003/0120924 (hereinafter US PGPub '924) and further in view of Baker in US PGPub No. 20070005962 (US PGPub '962).

3. For claim 1 and similar claims 10 and 19, US PGPub '924 discloses:

A method for confirming communication of data to a first device belonging to a first user from a second device belonging to a second user, the method comprising: (see [0018])

receiving a message containing data from the second device at the first device; (see [0027]: first channel)

and

allowing the first user and the second user to confirm a match between values from the first device and the corresponding values from the second device, wherein the confirmation process is performed through a separate communication channel, and wherein the confirmation ensures that the data sent by the second device is successfully received by the first device, is authentic, and is integrity-checked (see Abstract; [0031]; Figure 2) *but does not expressly disclose*:

...matching between the string of dictionary words from the first device and the corresponding string of dictionary words from the second device...,

translating the data into a string of words that can be recognized by a human;

allowing the second device to translate the data into a corresponding string of words;

displaying the string of dictionary words to the first user.

Baker however in US PGPub '962 does teach:

...matching between the string of dictionary words from the first device and the corresponding string of dictionary words from the second device..., (see [0060]: agree on key and derive dictionary word independently...)

translating the data into a string of words that can be recognized by a human; (see [0060]: dictionary of words or phrases...)

allowing the second device to translate the data into a corresponding string of words;

displaying the string of dictionary words to the first user (see [0060]: results translate in both directions...)

For claim 1 and similar claims 10 and 19, Immonen and Baker are analogous art because they are from the same field of endeavor. It would be obvious to one of ordinary skill in the art at the time of the invention to modify the process of integrity checking of a transmitted message as in Immonen such that integrity check values would be codebook data that would result in a translation to dictionary of words or phrases. The motivation for doing so would have been to ensure authenticated message transfer.

For claim 2 and similar claims 11 and 20, US PGPub '924 discloses wherein prior to receiving the message, the first device broadcasts a request asking for the second device's data, and wherein the data can be an identifier. (see [044] and [045])

For claim 3 and similar claims 12 and 21, US PGPub '924 discloses:

wherein the message received by the first device is signed with a private key corresponding to a public key associated with the second device; and

wherein the method further comprises using the public key associated with the second device to verify that the message is signed with the private key associated with the second device. (see [0054], lines 7 – 10)

For claim 4 and similar claims 13 and 22, US PGPub '924 discloses:

wherein while receiving the message, the first device receives more than one message; and

wherein the method further comprises translating the data in the other messages into strings of words which can be recognized by a human, and displaying these strings of words to the first user, thereby allowing the first user to match one of these strings of words with the corresponding string derived by the second device from the original data (see [0029]) *but does not expressly disclose* strings of dictionary words.

Baker however in US PGPub '962 does teach translating the data in the messages into strings of dictionary words (see [0060]: dictionary of words and phrases…results…codebook translates…)

For claim 5 and similar claims 14 and 23, US PGPub '924 discloses wherein prior to the reception of the message at the first device, the first user obtains a portion of the hash of the data on a separate communication channel and enters this portion into the first device, and wherein the first device uses this portion to filter subsequently received messages. (see [0043], authentication value; Figure 3 a & b)

For claim 6 and similar claims 15 and 24, US PGPub '924 discloses wherein the data received at the first device contains a cryptographically generated address (CGA) belonging to the second device, which is generated by:

performing a hash function on the second device's public key; and

constructing the CGA by combining a number of bits of an address belonging to the second device and a number of bits from the result of the hash function. (see [0045]; [0047): check code]

For claim 7 and similar claims 16 and 25, US PGPub '924 discloses:

wherein the message received by the first device includes a public key associated with the second device; and

wherein the method further comprises performing a hash function on the public key to verify the association between the CGA and the public key associated with the second device. (see [0045]; [0047])

For claim 9 and similar claims 18 and 27, US PGPub '924 discloses:

wherein the request includes a Crypto-Based Identifier (CBID) belonging to the first device; and

wherein the request is signed with a private key associated with the first device, thereby allowing the request to be verifiably associated with the first device. (see [0044]; lines 3 – 5)

Official Notice

4. For claim 8 and similar claims 17 and 26, US PGPub '924 discloses the method, medium and apparatus but does not expressly disclose wherein the translation uses a one-time password (OTP) dictionary.

Baker however in US PGPub '962 does teach wherein the translation uses a password dictionary (see [0060]) but does not expressly disclose the dictionary as a one-time password dictionary.

However the Examiner takes Official Notice of a one-time password dictionary.

It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the password dictionary of Baker such that it would be a one-time password dictionary since the Examiner takes Official Notice that this is a well known and obvious variant of a password dictionary.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Laurel Lashley whose telephone number is 571-272-0693. The examiner can normally be reached on Monday - Thursday, alt Fridays btw 7:30 am & 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Laurel Lashley
Examiner
Art Unit 2132
21 November 2007
LLL

Benjamin E. Lanier
Primary Examiner
Art Unit 2132